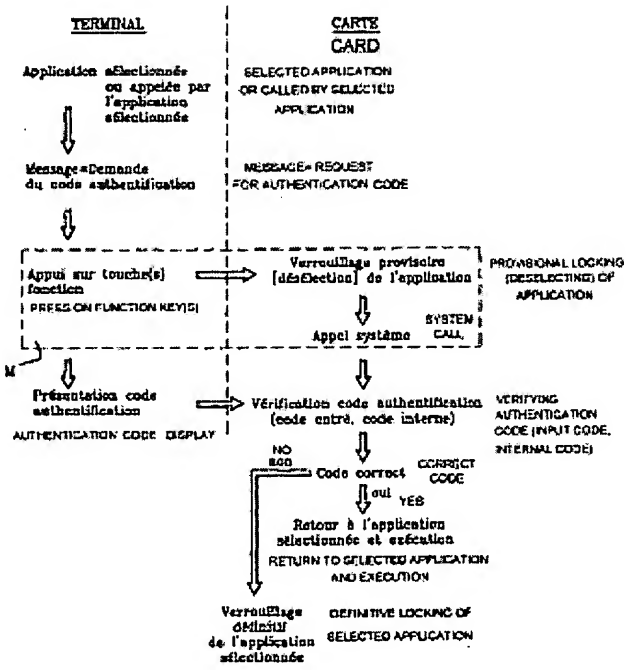
Protecting of multiple application smart card against fraud by using mechanism forcing access to presentation and verification interface of authentication string on demand of authentication string from terminal

Patent number: FR2804234
Publication date: 2001-07-27
Inventor: GIRARD PIERRE; BIDAN CHRISTOPHE
Applicant: GEMPLUS CARD INT (FR)
Classification:
- international: G06K19/073; G06K7/00; H04Q7/32
- european: G07F7/10D10M2; G07F7/10D6F
Application number: FR20000000829 20000124
Priority number(s): FR20000000829 20000124

Also published as:
WO0155980 (A1)
US2003079127 (A1)

Abstract of **FR2804234**

A smart card(s) includes an operating system and an interface for presentation and verification of an authentication string of a user. A system of the card uses a mechanism forcing the access to the presentation and verification interface of the authentication string when it initiates the process at the time of a demand of authentication string from a terminal. Independent claims are included for: (a) a multiple application smart card (b) a terminal capable of communication with a smart card



Data supplied from the ***esp@cenet*** database - Worldwide

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 804 234**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 00829**

(51) Int Cl[7] : **G 06 K 19/073**, G 06 K 7/00, H 04 Q 7/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24.01.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 27.07.01 Bulletin 01/30.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS Société en commandite par actions* — FR.

(72) **Inventeur(s) :** BIDAN CHRISTOPHE et GIRARD PIERRE.

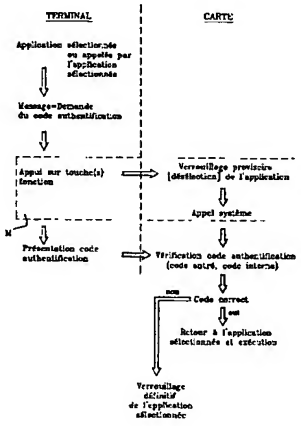
(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) PROCEDE DE PROTECTION CONTRE LE VOL DE LA VALEUR D'AUTHENTIFICATION POUR CARTES A PUCE(S) MULTI-APPLICATIONS, CARTES A PUCE(S) METTANT EN OEUVRE LE PROCEDE ET TERMINAUX SUSCEPTIBLES DE RECEVOIR LESDITES CARTES.

(57) L'invention concerne un procédé de protection contre le vol de la valeur d'authentification pour carte à puce (s) multi applications. Selon le procédé, il est prévu, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation et de vérification de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification.

L'invention s'applique à des terminaux (T) susceptibles de communiquer avec des cartes à puces (C) comprenant à cette fin au moins une touche fonction (P_{IN}) ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.



FR 2 804 234 - A1

PROCEDE DE PROTECTION CONTRE LE VOL DE LA VALEUR D'AUTHENTIFICATION POUR CARTES A PUCE(S) MULTI-APPLICATIONS, CARTES A PUCE(S) METTANT EN ŒUVRE LE PROCEDE ET TERMINAUX SUSCEPTIBLES DE RECEVOIR LESDITES CARTES

L'invention concerne un procédé de protection contre le vol de la valeur d'authentification pour les cartes à puce(s) multi applications aptes à communiquer avec l'extérieur au moyen d'un terminal. Elle concerne également les cartes à puce(s) mettant en œuvre ledit procédé et les terminaux susceptibles de recevoir lesdites cartes. L'invention s'applique tout particulièrement aux cartes à puces multi applications utilisées avec les téléphones mobiles tels que les téléphones définis par le standard GSM.

On entend par cartes à puce(s) multi-applications des cartes contenant une ou plusieurs puces de circuit intégré lesdites cartes étant destinées à pouvoir exécuter différents programmes d'application chargés ou téléchargés au cours de la vie de la carte.

Parmi les solutions de cartes multi-applications existantes à ce jour, nous pouvons signaler « JavaCard » défini par Sun ou « SmartCard for Windows » défini par Microsoft.

Pour simplifier, on parlera dans la suite d'applications pour désigner les programmes d'applications (ou Applet en terminologie anglo saxonne).

On entend par valeur d'authentification, que l'on dénomme également code d'authentification, une valeur permettant d'authentifier le titulaire de la carte. La

valeur d'authentification peut être une donnée connue du titulaire seul (en général, un numéro d'identification personnel ou PIN- Personnal Identifier Number), déduite d'une caractéristique biométrique du titulaire (par exemple, voix, empreinte digitale, chaleur…) ou résultant d'une action que seul le titulaire peut effectuer (par exemple, signature).

Pour des raisons de compatibilité avec les cartes à puce(s) ne supportant qu'une unique application, et de simplicité pour l'utilisateur de la carte, les cartes à puce multi-applications ont généralement une seule valeur d'authentification pour toutes les applications. Ainsi, la spécification OP définie par VISA, et qui tient lieu actuellement de standard pour le chargement/téléchargement et la gestion interne d'applications sur les cartes à puce multi-applications, définit un unique PIN global pour toutes les applications résidentes et futures de la carte.

Le problème soulevé par le déposant dans le cas d'une carte multi-applications, vient de ce que la carte est prévue pour pouvoir charger ou télécharger de nouvelles applications pendant toute sa vie. A priori ceci est un avantage, mais en pratique cette caractéristique rend la carte vulnérable, car des applications malveillantes pourront être chargées avec d'autres applications de manière transparente vis à vis du titulaire. C'est donc une porte ouverte à de telles applications qui bien sûr en pratique vont chercher à découvrir la valeur d'authentification de la carte.

Suite à cette observation, le déposant a identifié une attaque permettant de trouver la valeur d'authentification de la carte.

Cette attaque suppose l'existence d'une application malveillante possédant un accès vers l'extérieur.

Une application possède un accès vers un terminal dès lors qu'il existe un terminal permettant à l'application de directement dialoguer avec l'utilisateur via ce terminal. On peut citer par exemple dans le cadre du GSM les applications pouvant modifier les menus affichés sur le téléphone mobile.

Voici alors la procédure suivie lors de cette attaque au moyen d'une application qui peut dialoguer avec l'extérieur.

En fait, l'application utilise sa capacité à dialoguer avec l'extérieur pour simuler sur le terminal l'interface qui permet de demander à l'utilisateur d'entrer la valeur d'authentification.

En effet, la vérification de l'identité de l'utilisateur de la carte est généralement réalisée par l'intermédiaire d'une application en charge d'afficher, sur l'écran du terminal dans lequel est insérée la carte à puce(s), un menu invitant l'utilisateur de présenter la valeur d'authentification. Une fois la valeur d'authentification présentée, le terminal retourne cette valeur à ladite application qui vérifie (éventuellement par l'intermédiaire d'une application en charge de la vérification de la valeur d'authentification) que la valeur présentée par l'utilisateur est identique à la valeur d'authentification de la carte. Si tel est le cas, l'application répond par l'affirmation ; par la négation dans le cas contraire.

L'accès à l'application en charge de l'affichage, sur l'écran du terminal dans lequel est insérée la carte à puce(s), du menu invitant l'utilisateur à présenter la valeur d'authentification est généralement contrôlée afin que seules les applications autorisées

puissent initier la vérification de la valeur d'authentification.

Néanmoins, une application malveillante possédant un accès vers un terminal peut simuler sur ce terminal le menu invitant l'utilisateur à présenter sa valeur d'authentification. L'utilisateur va alors en toute confiance présenter sa valeur d'authentification, permettant ainsi à l'application malveillante de découvrir cette valeur. Par la suite, l'application malveillante pourra, grâce à sa capacité de dialoguer vers l'extérieur, fournir la valeur d'authentification au développeur de l'application malveillante. Ceci sera d'autant plus facile dans le cas d'un terminal tel qu'un téléphone mobile pour lequel l'application malveillante pourra composer un numéro afin de communiquer la valeur d'authentification.

La présente invention a pour but de remédier à ces problèmes.

La présente invention a pour objet un procédé de protection contre le vol de la valeur d'authentification pour carte à puce(s) multi applications comprenant un système d'exploitation, principalement caractérisé en ce qu'il comprend, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification.

Selon une autre caractéristique, le mécanisme comporte la réservation sur le terminal d'au moins une touche fonction ou d'une séquence de touches fonction

apte à provoquer un appel du système d'exploitation de la carte.

La mise en œuvre du mécanisme comprend la séquence d'actions suivantes :

- l'appui sur la ou les touches fonction par l'utilisateur de la carte pour autoriser la présentation de la valeur d'authentification et provoquer un verrouillage provisoire des applications de la carte,
- la présentation de la valeur d'authentification,
- la mise en œuvre de la procédure de vérification de la valeur d'authentification par le système d'exploitation après les deux premières actions.

L'invention concerne également une carte à puce(s) multi applications comprenant un système d'exploitation et des moyens de communication avec un terminal, principalement caractérisé en ce qu'elle comprend des moyens pour que les appels système en provenance du terminal pour la présentation de la valeur d'authentification ne puissent être intercepter par les applications.

L'invention concerne un terminal susceptible de communiquer avec une carte à puce(s), principalement caractérisé en ce qu'il comprend au moins une touche fonction ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.

Le terminal pourra être un téléphone mobile par exemple du type GSM.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci après et en regard des dessins sur lesquels :

- la figure 1 représente le schéma illustrant la mise en œuvre du procédé selon l'invention,
- la figure 2 représente le schéma d'un terminal susceptible de communiquer avec une carte à puce(s) selon l'invention,
- la figure 3 représente le schéma d'une carte multi application selon l'invention.

Une réalisation pratique du procédé selon l'invention va être décrite dans la suite en regard de la figure 1.

Le procédé comprend un verrouillage provisoire de l'application sélectionnée par l'utilisateur ou d'une application appelée par l'application sélectionnée par cet utilisateur ; un appel du système d'exploitation de la carte à puce(s) pour la mise en œuvre par le système d'exploitation de la procédure de vérification de la valeur d'authentification.

Selon la réalisation proposée, le verrouillage est obtenu par l'association d'une touche fonction ou d'une séquence de touches prévue sur le terminal pour pouvoir initier la présentation de la valeur d'authentification et un appel système déclenché par l'appui de cette touche fonction ou de la séquence de touches fonction. Dès lors que l'utilisateur voie apparaître un message de demande de la valeur d'authentification sur l'écran du terminal, il ne peut poursuivre la procédure de présentation de la valeur d'authentification qu'après avoir appuyé sur ladite touche, garantissant de cette manière que la procédure de vérification de la valeur d'authentification est effectuée par le système d'exploitation ou sous son contrôle.

En effet, lorsqu'une application s'exécute au sein de la carte et que le menu de présentation de la valeur d'authentification apparaît sur l'écran du terminal,

l'utilisateur doit appuyer sur la touche fonction prévue portant la référence P_{IN} sur les schémas (ou sur la séquence de touches fonction) pour présenter sa valeur d'authentification. Cette action permet de verrouiller provisoirement l'application en cours d'exécution (c'est à dire que l'application est suspendue) et de lancer un appel vers le système d'exploitation de la carte. C'est alors sous le contrôle du système d'exploitation qu'est effectuée la procédure de présentation et de vérification de la valeur d'authentification. Cette vérification consiste à comparer la valeur d'authentification présentée par l'utilisateur avec la valeur d'authentification mémorisée dans la carte.

Lorsque la valeur d'authentification présentée par l'utilisateur est correcte, le système d'exploitation de la carte déverrouille l'application en cours d'exécution qui peut alors reprendre son exécution à l'endroit où elle a été suspendue ; dans le cas contraire, le système d'exploitation affiche un message d'erreur et exécute les actions de sécurité adéquates (par exemple verrouiller définitivement l'application et afficher un message d'alerte).

La figure 2 illustre un terminal T apte à communiquer avec une carte à puce(s). Ce terminal possède de manière connue une unité centrale de traitement UC avec une mémoire de programme MPT. Cette mémoire comporte une interface IT de communication avec les cartes à puce(s) classique en soi. Seule une modification est prévue pour permettre au terminal de se mettre en attente de l'appui sur la touche P_{IN} (ou la séquence de touches fonction) après l'affichage du message de demande de la valeur d'authentification et

d'envoyer un appel au système d'exploitation de la carte.

Une carte à puce(s) C multi applications a été schématisée sur la figure 3 afin d'illustrer les différents éléments entrant dans la mise en œuvre du procédé conforme à l'invention. Prenons le cas pour simplifier où une seule puce P de circuit intégré est présente dans la carte, il s'agit d'une puce contenant un ou plusieurs microprocesseur(s) et ses mémoires associées en particulier une mémoire de programmes MPC. Cette mémoire contient le système d'exploitation et l'interface de présentation et de vérification de la valeur d'authentification. En général une autre mémoire de programmes MPA est destinée à mémoriser les différents programmes d'applications A1, A2,… An.

REVENDICATIONS

1.Procédé de protection contre le vol de la valeur d'authentification pour carte à puce(s) multi applications comportant un système d'exploitation et une interface de présentation et de vérification de la valeur d'authentification de l'utilisateur de ladite carte, caractérisé en ce qu'il comprend, pour empêcher une application possédant un accès vers un terminal de simuler le menu invitant l'utilisateur à présenter la valeur d'authentification, un mécanisme forçant l'accès à l'interface de présentation et de vérification de la valeur d'authentification par le système d'exploitation de la carte quelle que soit l'application ayant initié le processus, dès lors qu'il y a une demande de valeur d'authentification.

2. Procédé de protection contre le vol de la valeur d'authentification selon la revendication 1, caractérisé en ce que le mécanisme comporte la réservation sur le terminal d'au moins une touche fonction ou d'une séquence de plusieurs touches fonction apte à provoquer un appel du système d'exploitation de la carte.

3. Procédé de protection contre le vol de la valeur d'authentification selon la revendication 1 ou 2, caractérisé en ce que la mise en œuvre du mécanisme comprend la séquence d'actions suivantes :

- l'appui sur la ou les touches fonction par l'utilisateur de la carte pour autoriser la présentation de la valeur d'authentification et provoquer un verrouillage provisoire de l'application,
- la présentation de la valeur d'authentification,

- la mise en œuvre de la procédure de vérification de la valeur d'authentification par le système d'exploitation après les deux premières actions.

4. Carte à puce(s) multi applications comprenant un système d'exploitation et des moyens de communication avec un terminal, caractérisé en ce qu'elle comprend des moyens (MPC) pour que les appels système en provenance du terminal (T) pour la présentation de la valeur d'authentification ne puissent être interceptés par les applications de la carte.

5. Terminal susceptible de communiquer avec une carte à puce(s), caractérisé en ce qu'il comprend au moins une touche fonction (P_{IN}) ou une séquence de touches fonction réservée pour effectuer un appel système à la carte et initier la présentation de la valeur d'authentification.

6. Terminal selon la revendication 5, caractérisé en ce qu'il est constitué par un téléphone mobile.

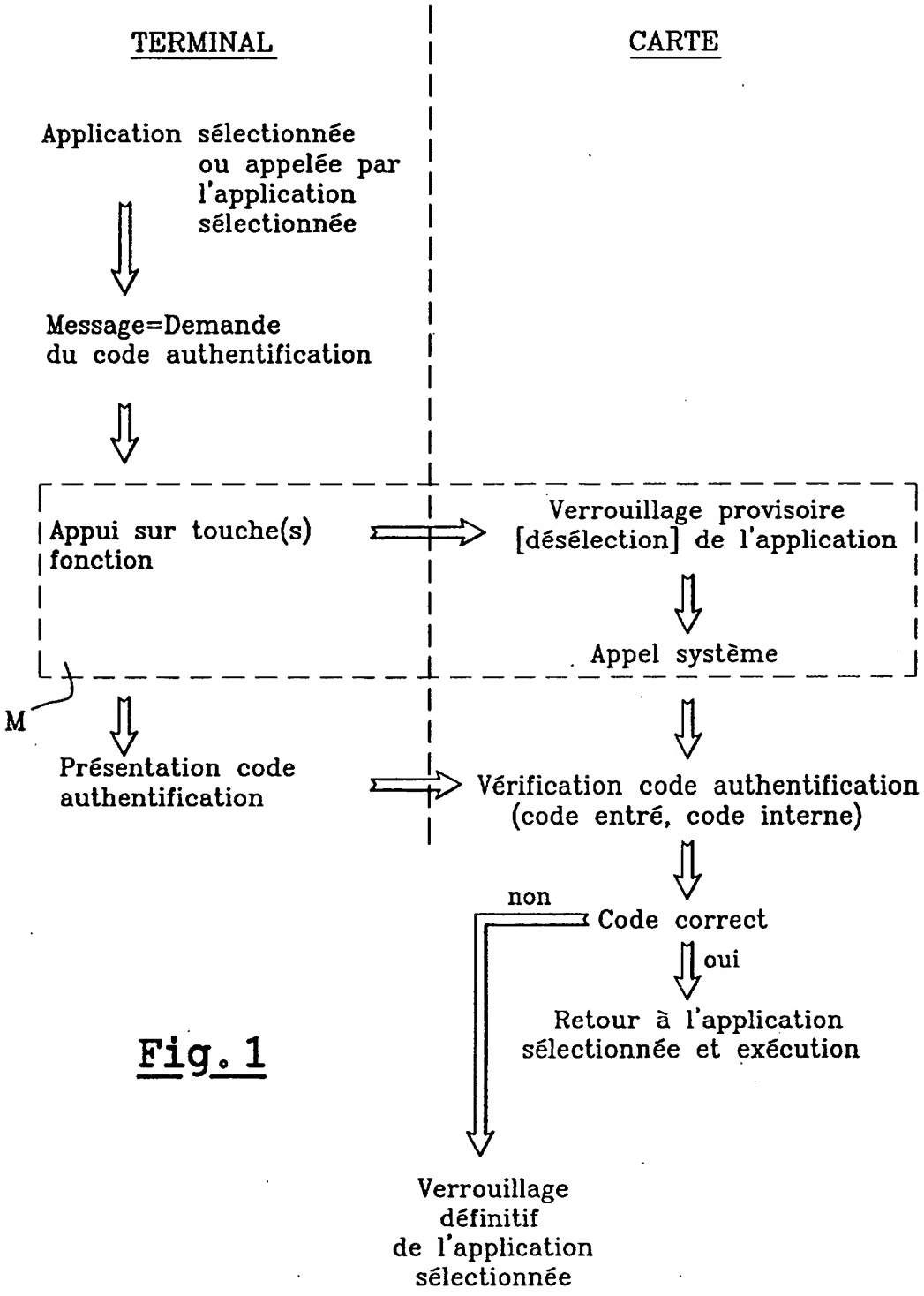

TERMINAL
CARTE
Application sélectionnée ou appelée par l'application sélectionnée
Message=Demande du code authentification
Appui sur touche(s) fonction
Verrouillage provisoire [désélection] de l'application
Appel système
M
Présentation code authentification
Vérification code authentification (code entré, code interne)
non
Code correct
oui
Retour à l'application sélectionnée et exécution
Verrouillage définitif de l'application sélectionnée

Fig. 1

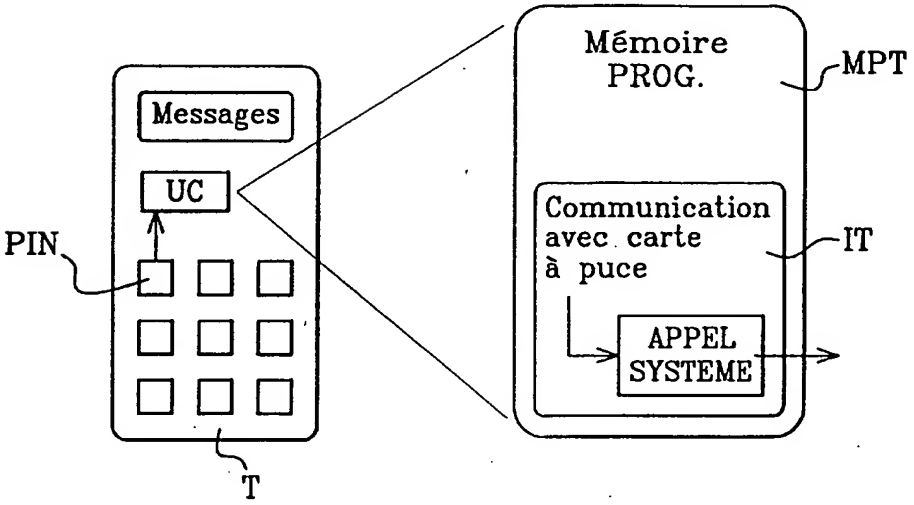

Mémoire
PROG.
MPT
Messages
UC
PIN
Communication
avec carte
à puce
IT
APPEL
SYSTEME
T

Fig. 2

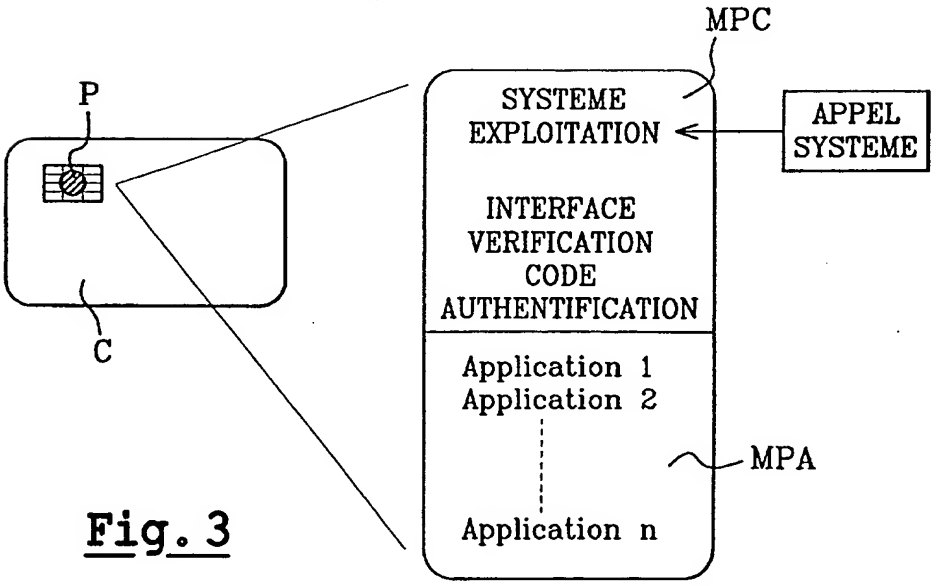

MPC
P
SYSTEME
EXPLOITATION
APPEL
SYSTEME
INTERFACE
VERIFICATION
CODE
AUTHENTIFICATION
Application 1
Application 2
MPA
Application n
C

Fig. 3

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2804234

N° d'enregistrement national

FA 584054
FR 0000829

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	EP 0 325 776 A (IBM) 2 août 1989 (1989-08-02) * page 3, ligne 5 - ligne 49 *	1-6	G06K19/073 G06K7/00 H04Q7/32
Y	US 6 005 942 A (CHAN ALFRED ET AL) 21 décembre 1999 (1999-12-21) * colonne 3 - colonne 6 *	1-6	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			G07F

Date d'achèvement de la recherche: 23 octobre 2000

Examinateur: Wolles, B

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

1